CENTRE CANADIEN POUR LA
CYBERSÉCURITÉ

Introduction à l'environnement de cybermenace

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

À PROPOS DU PRÉSENT DOCUMENT

Le présent document décrit les concepts pertinents aux discussions relatives aux activités de cybermenace dans le contexte canadien et sert de point de référence aux publications du Centre canadien pour la cybersécurité (CCC). Il transmet des connaissances de base sur l'environnement de cybermenace, notamment sur les auteurs de cybermenace et leurs motivations, le degré de sophistication, les techniques, les outils et l'exposition aux cybermenaces.

Prière de consulter le glossaire du CCC pour des termes additionnels, ainsi que les blogues pour de plus amples discussions sur l'environnement de cybermenace.

CYBERMENACE

Une **cybermenace** est une activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient.

Par **environnement de cybermenace**, on entend l'espace virtuel où les auteurs de cybermenace mènent des activités de cybersécurité malveillantes.

AUTEURS DE CYBERMENACE

Les **auteurs de cybermenace** sont des États, des groupes ou des personnes qui cherchent à tirer avantage des vulnérabilités, d'une sensibilisation insuffisante à la cybersécurité et des progrès technologiques pour obtenir un accès non autorisé aux systèmes d'information ou encore porter préjudice aux données, aux dispositifs, aux systèmes et aux réseaux des victimes. L'universalisation d'Internet a fait en sorte que ces auteurs de menace peuvent compromettre, peu importe où ils se trouvent dans le monde, la sécurité des systèmes d'information au Canada.

MOTIVATIONS

On peut catégoriser les auteurs de cybermenace selon leur motivation et, dans une certaine mesure, selon leur degré de sophistication. Les auteurs de menace cherchent à obtenir accès aux dispositifs, à la puissance de traitement, aux ressources informatiques et à l'information pour toutes sortes de raison. Or, chaque type d'auteurs de cybermenace est animé par une motivation principale.

Figure 1 : Auteurs de cybermenace

AUTEUR DE CYBERMENACE	MOTIVATION
ÉTATS-NATIONS	GÉOPOLITIQUE
CYBERCRIMINELS	GAINS FINANCIERS
HACKTIVISTES	IDÉOLOGIQUE
GROUPES TERRORISTES	VIOLENCE IDÉOLOGIQUE
AMATEURS DE SENSATIONS FORTES	SATISFACTION
MENACES INTERNES	MÉCONTENTEMENT

SOPHISTICATION

Les auteurs de cybermenace n'ont pas les mêmes capacités et le même degré de sophistication. Ils tirent parti d'un large éventail de ressources, de formation et de soutien pour mener leurs activités. Ils peuvent agir seuls ou faire partie d'une organisation plus large (p. ex. le programme de renseignement d'un État-nation ou un groupe du crime organisé). Des auteurs sophistiqués ont parfois recours à des outils et techniques plus rudimentaires et accessibles au public, puisqu'ils permettent d'accomplir efficacement une tâche donnée ou qu'ils rendent le processus d'attribution plus difficile pour les responsables de la sécurité.

Les **États-nations** sont souvent les auteurs de cybermenace les plus sophistiqués en raison des ressources et du personnel à leur disposition, et des efforts de planification et de coordination qu'ils peuvent déployer. Certains États-nations entretiennent des relations opérationnelles avec des membres du crime organisé.

Les **cybercriminels** sont généralement considérés comme ayant un niveau moyen de sophistication par rapport aux États-nations. Ils peuvent tout de même disposer de fonctions de planification et de soutien, ainsi que de capacités techniques spécialisées susceptibles de faire de nombreuses victimes.

Les auteurs de cybermenace ayant un niveau de sophistication et de compétence plus élevé sont souvent appelés des **menaces persistantes avancées (MPA)**, car ils sont en mesure d'utiliser des techniques avancées pour mener des campagnes complexes et prolongées afin de réaliser leurs objectifs stratégiques. Cette dénomination est généralement réservée aux États-nations et aux groupes du crime organisé très compétents.

Les **hacktivistes**, les **groupes terroristes** et les **amateurs de sensations fortes** sont généralement moins sophistiqués. Ils ont souvent recours à des outils accessibles à grande échelle qu'il est facile de déployer avec des compétences techniques limitées. Bien souvent, leurs actions n'ont aucune conséquence durable sur leurs cibles, abstraction faite du tort causé à leur réputation.

Les **menaces internes** proviennent des personnes qui travaillent dans l'organisation. Elles sont particulièrement dommageables puisque ces personnes ont accès aux réseaux internes qui sont protégés par des périmètres de sécurité. Comme l'accès est un facteur essentiel pour les auteurs de menace malveillants, le fait d'avoir un accès privilégié élimine le besoin de faire appel à d'autres moyens. Les menaces internes sont associées à l'un des types d'auteurs de menace mentionnés précédemment et peuvent également inclure les employés mécontents qui cherchent à se venger.

ACTIVITÉS DE CYBERMENACE

Les auteurs de cybermenace mènent leurs activités malveillantes de différentes façons, que ce soit en exploitant des vulnérabilités techniques, en utilisant des techniques de piratage psychologique ou en manipulant les médias sociaux. Un adversaire déterminé et compétent choisira souvent la technologie la plus susceptible de mener à une exploitation fructueuse des systèmes d'une cible après avoir pratiqué des activités de reconnaissance et pourrait faire appel à une gamme de techniques pour arriver à ses fins. Or, la majorité des auteurs de menace ratissent plus large dans l'espoir d'exploiter n'importe quels réseaux ou bases de données non sécurisés.

Les **vulnérabilités techniques** sont des lacunes ou des défauts dans la conception, la mise en œuvre, l'exploitation ou la gestion d'un système de technologie de l'information (TI), d'un dispositif ou d'un service qui peuvent fournir un accès aux auteurs de cybermenace. Par exemple, un auteur de menace peut tenter d'installer un logiciel malveillant, appelé **maliciel**, ou tirer avantage de failles existantes pour exploiter le système ciblé. En plus de l'installation de maliciels, les auteurs de menace utilisent également des outils qui exploitent directement des vulnérabilités techniques en particulier.

Le **piratage psychologique** se compose des méthodes d'exploitation qui ciblent les vulnérabilités humaines comme la négligence et une confiance aveugle. Les auteurs de menace font appel au piratage psychologique pour inciter quelqu'un à donner accidentellement accès à un système, un réseau ou un dispositif. L'hameçonnage et le harponnage sont des techniques de piratage psychologique courantes. (Prière de consulter l'*Annexe : Les outils de l'auteur de cybermenace* pour de plus amples renseignements.)

Les auteurs de cybermenace étrangers peuvent également manipuler les médias sociaux, la publicité légitime et les outils d'échange d'information pour mener des campagnes **d'influence étrangère en ligne** en vue d'affecter de façon générale des événements à l'échelle nationale comme une élection, un recensement ou une campagne de santé publique, ainsi que des débats publics.

Ils tirent avantage de leur compréhension du fonctionnement des médias traditionnels et des médias sociaux – et de la façon dont les personnes consomment l'information – pour diffuser leur message à un auditoire plus large, et à un coût relativement bas. Ils peuvent y parvenir en se faisant passer pour des fournisseurs d'information légitimes, en piratant des comptes dans les médias sociaux, ou en créant des sites Web et de nouveaux comptes.

Par **attribution**, on entend l'action de déterminer avec précision quel est l'auteur de menace responsable d'un ensemble d'activités en particulier. L'attribution d'une activité à un auteur de cybermenace est importante pour plusieurs raisons, notamment pour assurer la défense d'un réseau, appliquer la loi, prendre des mesures dissuasives et préserver des relations étrangères. Or, cette attribution peut s'avérer difficile puisque de nombreux auteurs de cybermenace ont recours à l'obscurcissement pour éviter que des activités ne leur soient attribuées.

Par **obscurcissement**, on entend les outils et les moyens que les auteurs de menace utilisent pour dissimuler leur identité, leurs objectifs, leurs techniques et même leurs victimes. Pour éviter de laisser aux responsables de la sécurité des indices susceptibles de les aider à attribuer l'activité, les auteurs de menace emploient des outils et techniques facilement accessibles ou des outils personnalisés qui permettent de transmettre secrètement l'infor mation sur Internet.

Les auteurs de menace sophistiqués peuvent également mener une attaque **sous faux pavillon**, une technique qui consiste à imiter les activités connues d'autres auteurs de menace dans l'espoir que les responsables de la sécurité attribuent faussement l'activité à quelqu'un d'autre. Par exemple, un État-nation pourrait employer un outil utilisé par des cybercriminels.

La capacité des auteurs de cybermenace de dissimuler leurs actions dépend de leur degré de sophistication et de leur motivation. En règle générale, les États-nations et les cybercriminels compétents arrivent plus habilement à pratiquer l'obscurcissement que d'autres auteurs de cybermenace.

EXPOSITION AUX CYBERMENACES

L'exposition aux cybermenaces fait référence à tous les points terminaux qu'un auteur de menace peut tenter d'exploiter sur des dispositifs connectés à Internet dans un contexte de cybermenace. Parmi les cibles et vecteurs de menace possibles, on retrouve également plusieurs processus utilisés pour produire et mettre en œuvre des systèmes d'information connectés à Internet, ou qui dépendent de tels systèmes. Les services, les dispositifs et les données peuvent tous être ciblés afin de compromettre les systèmes de production et de livraison, comme les chaînes d'approvisionnement et les systèmes de gestion des services. L'exposition aux menaces augmentera à mesure que ces processus continueront d'évoluer.

De plus, les systèmes qui connectent des entités physiques avec Internet sont devenus de plus en plus courants. Par exemple, le réseau électrique intelligent, les dispositifs de l'Internet des objets (IdO) et les systèmes de contrôle industriels présentent un risque de voir les auteurs de cybermenace s'ingérer dans un contexte physique.

Les applications et les dispositifs connectés à Internet procurent des avantages considérables aux utilisateurs et à l'économie mondiale. Or, lorsqu'un plus grand nombre d'actifs matériels et informationnels seront accessibles en ligne ou comporteront une composante numérique, les auteurs de cybermenace auront davantage d'occasions de mener des activités de cybermenace malveillantes, d'accéder à l'information, de nuire aux opérations ou de causer des dommages matériels.

ANNEXE : LES OUTILS DE L'AUTEUR DE CYBERMENACE

Le présent document n'a pas pour objectif de décrire toutes les cybercapacités que les auteurs de menace peuvent déployer. Vous trouverez ci-dessous une liste non exhaustive des outils et techniques couramment utilisés par les auteurs de menace. Pour simplifier, les éléments apparaissent en ordre alphabétique et non en fonction de leur fréquence ou de leur incidence.

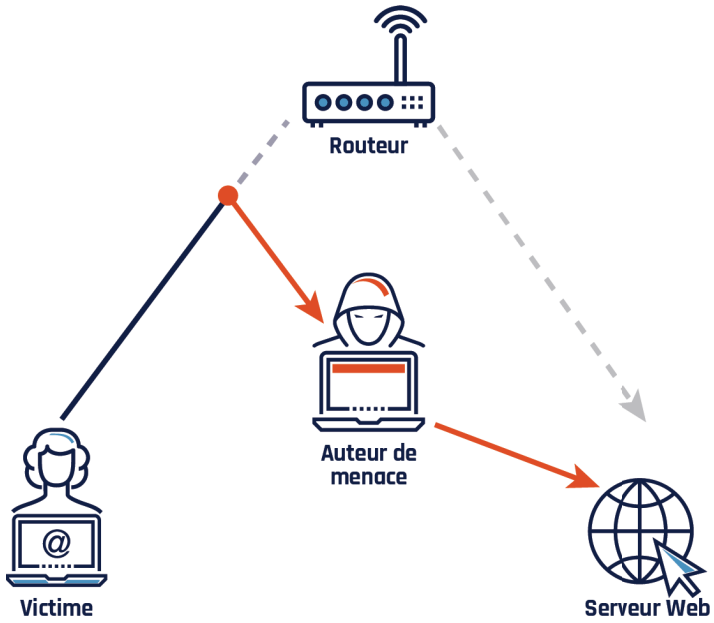
ATTAQUE DE BOURRAGE DE JUSTIFICATIFS [Credential Stuffing]

Par attaque de bourrage de justificatifs, on entend une manœuvre consistant à utiliser des listes de combinaisons de noms d'utilisateur et de mots de passe compromis afin d'accéder frauduleusement à des comptes en ligne. Les auteurs de cybermenace ont recours à ces listes pour lancer des demandes de connexion automatisées à grande échelle dans l'espoir qu'une des combinaisons corresponde à un compte existant auquel ils pourront avoir accès.

ATTAQUE DE L'INTERCEPTEUR [Person-in-the-middle]

L'**attaque de l'intercepteur (PITM pour *Person-in-the-middle*)** est une technique qui consiste à intercepter les communications entre deux parties, comme un utilisateur et un serveur Web, à l'insu de la victime qui croit avoir établi une connexion directe et sécurisée avec un site Web. L'attaque de l'intercepteur permet aux auteurs de menace de surveiller les communications, de réacheminer le trafic, de modifier l'information, d'installer des maliciels et d'obtenir des renseignements nominatifs ou de l'information sensible. Elle peut être réalisée au moyen de diverses techniques : l'hameçonnage, le dévoiement, le typosquattage, l'écoute électronique par réseau Wi-Fi et le détournement SSL.

Figure 2 : Attaque de l'intercepteur



ATTAQUE PAR TÉLÉCHARGEMENT FURTIF ET ATTAQUE DE POINT D'EAU [Drive-By Exploit and Watering Hole]

Par **attaque par téléchargement furtif**, on entend le code malveillant qu'un auteur de cybermenace installe sur un site Web à l'insu de l'hôte dans le but de compromettre les dispositifs des utilisateurs qui le consultent. Un **point d'eau** est un site Web compromis au moyen d'un exploit et fréquenté par des personnes spécifiquement ciblées par un auteur de cybermenace.

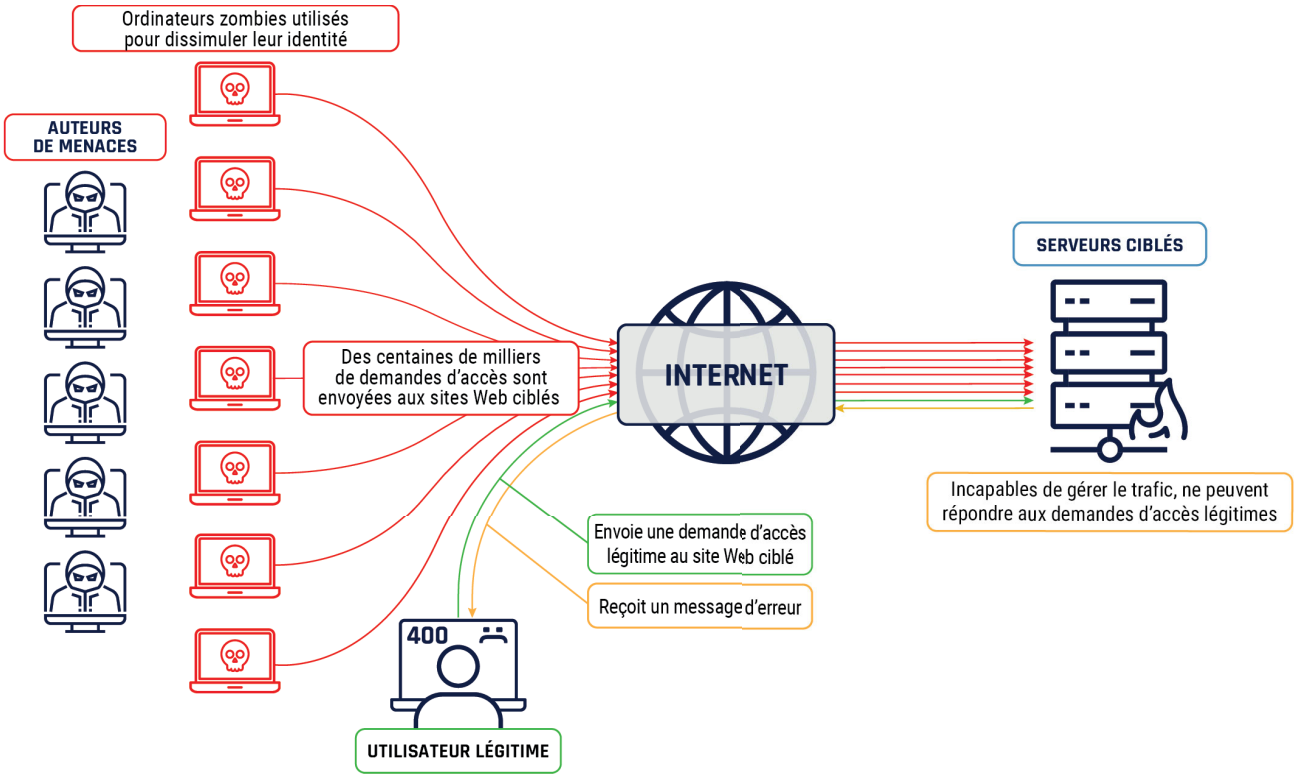
CRYPTOMINAGE [Cryptomining]

Par **cryptominage** ou minage de cryptomonnaie, on entend le processus selon lequel des programmes informatiques utilisent la puissance de calcul d'ordinateurs pour générer ou « miner » de la cryptomonnaie, activité pour laquelle le mineur reçoit, pour ses services, une fraction de la cryptomonnaie minée. Le **cryptominage pirate** permet à un auteur de menace d'exploiter secrètement le dispositif d'une victime (p. ex. des ordinateurs, des appareils mobiles et les dispositifs de l'IdO) dans le but de miner de la cryptomonnaie sans autorisation. Pour accroître son efficacité (c.-à-d. ses revenus), l'auteur de menace peut faire appel à un réseau de zombies composé de dispositifs compromis. Les logiciels malveillants utilisés à cette fin sont généralement téléchargés lors de la consultation d'un site Web compromis, à l'installation d'une application ou par hameçonnage.

DÉNI DE SERVICE (DISTRIBUÉ) [(Distributed) Denial of Service]

Le **déni de service (DoS pour *Denial of Service*)** est une technique qu'utilisent les auteurs de menace pour tenter d'interrompre les activités habituelles d'un hôte en particulier (p. ex. site Web, serveur, réseau, Internet des objets) en le surchargeant de demandes d'accès. L'objectif général est de rendre l'hôte inaccessible aux demandes d'accès légitimes des utilisateurs et de rendre le système ciblé inopérant. Les **attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*)** ajoutent un degré de complexité, puisqu'elles consistent à inonder de messages des sites Web à partir de sources multiples (p. ex. des réseaux de zombies). Il est d'ailleurs fort difficile d'arrêter ces activités d'envergure et de faire la distinction entre le trafic généré par les utilisateurs légitimes et le trafic malveillant.

Figure 3 : Déni de service distribué



DÉTOURNEMENT SSL [SSL Hijacking]

Le **détournement SSL (Secure Sockets Layer)** est une technique par laquelle un auteur de menace cherche à intercepter et à rediriger une connexion non sécurisée entre une victime et un serveur tentant d'établir une connexion sécurisée. La connexion sécurisée est alors fournie par l'auteur de menace plutôt que par le site Web prévu, ce qui lui permet d'intercepter et de compromettre les communications à l'insu de la victime (voir *l'attaque de l'intercepteur*). Le détournement SSL n'a pas pour objet de porter atteinte à la sécurité fournie par le procotole SSL, mais bien de compromettre la connexion entre les parties non chiffrée et chiffrée de la communication.

DÉTOURNEMENT DE FORMULAIRE [Formjacking]

Le détournement de formulaire consiste à permettre à des cybercriminels d'injecter du code malveillant dans un formulaire de page Web, comme une page de paiement, pour le compromettre et voler les détails relatifs aux cartes de crédit ainsi que d'autres renseignements que les utilisateurs entrent sur ces pages.

DÉVOIEMENT [Pharming]

Le dévoiement est une technique qui consiste à rediriger le trafic d'un site Web légitime vers un site malveillant. Pour réaliser cette supercherie, les auteurs de menace modifient les paramètres système de l'utilisateur ou exploitent les vulnérabilités logicielles du serveur du système d'adressage par domaines (DNS pour *Domain Name System*) qui assure la correspondance entre les adresses URL et les adresses IP. Contrairement au typosquattage (voir ci-dessous), une technique qui tire avantage des fautes de frappe de l'utilisateur pour le rediriger vers un site Web illégitime, le dévoiement peut rediriger l'utilisateur malgré le fait qu'il ait tapé la bonne adresse URL. Du premier coup d'œil, le site Web illégitime peut sembler légitime, alors qu'il sert en réalité à installer un maliciel et à obtenir des renseignements nominatifs ou de l'information sensible.

DISSIMULATEUR D'ACTIVITÉ [Rootkit]

Un **dissimulateur d'activité** est une application malveillante conçue pour fournir secrètement à un auteur de menace un accès racine ou administrateur privilégié aux logiciels et aux systèmes qui se trouvent sur le dispositif d'un utilisateur. Un dissimulateur d'activité fournit un accès complet, y compris la capacité de modifier les logiciels utilisés pour détecter les maliciels. Il peut être installé de différentes façons, notamment par perçage du mot de passe, par piratage psychologique, ou encore en tirant avantage d'un bogue ou d'un défaut de conception qui accorde un accès privilégié au système ou au dispositif d'un utilisateur.

ÉCOUTE ÉLECTRONIQUE PAR RÉSEAU WI-FI [Wi-Fi Eavesdropping]

Un auteur de menace utilise l'**écoute électronique par réseau Wi-Fi** pour installer ce qui semble être un point d'accès Wi-Fi légitime dans une zone publique. Les utilisateurs qui se connectent à un tel point d'accès, que l'on appelle souvent un point d'accès malveillant ou indésirable, peuvent alors être victimes d'une attaque de l'intercepteur. Une telle activité permet à un auteur de menace de surveiller les communications et d'obtenir des renseignements nominatifs ou de l'information sensible.

EFFACEURS [Wiper]

Les **effaceurs** sont des maliciels conçus pour détruire entièrement le disque dur des dispositifs infectés.

EXPLOITS ET TROUSSES D'EXPLOIT [Exploits and Exploit Kits]

Un **exploit** est un code malveillant qui permet de tirer avantage d'une vulnérabilité non corrigée. Une **trousse d'exploit** est une collection d'exploits qui ciblent les applications logicielles non sécurisées. Les trousses d'exploit sont adaptées de manière à chercher des vulnérabilités spécifiques et à exécuter l'exploit correspondant à la vulnérabilité relevée. Si un utilisateur visite un site Web hébergeant une trousse d'exploit, celle-ci comparera son référentiel d'exploits aux applications logicielles qui se trouvent sur le dispositif de l'utilisateur, et déploiera l'exploit correspondant à la vulnérabilité décelée.

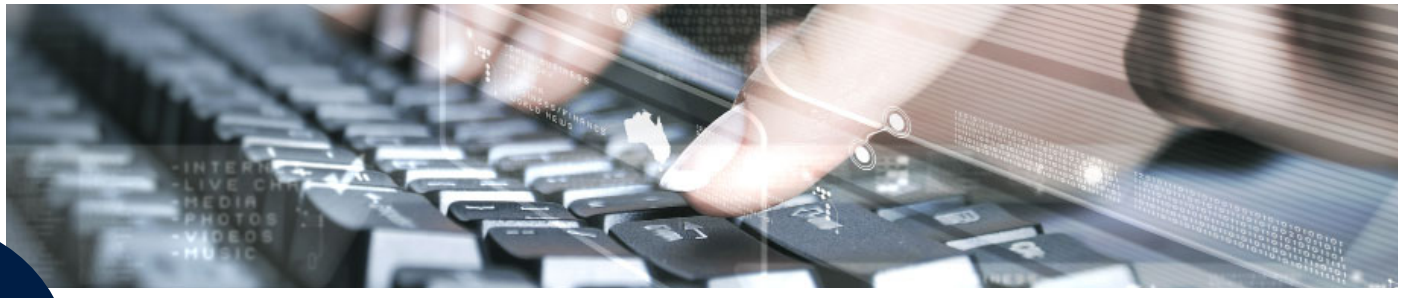
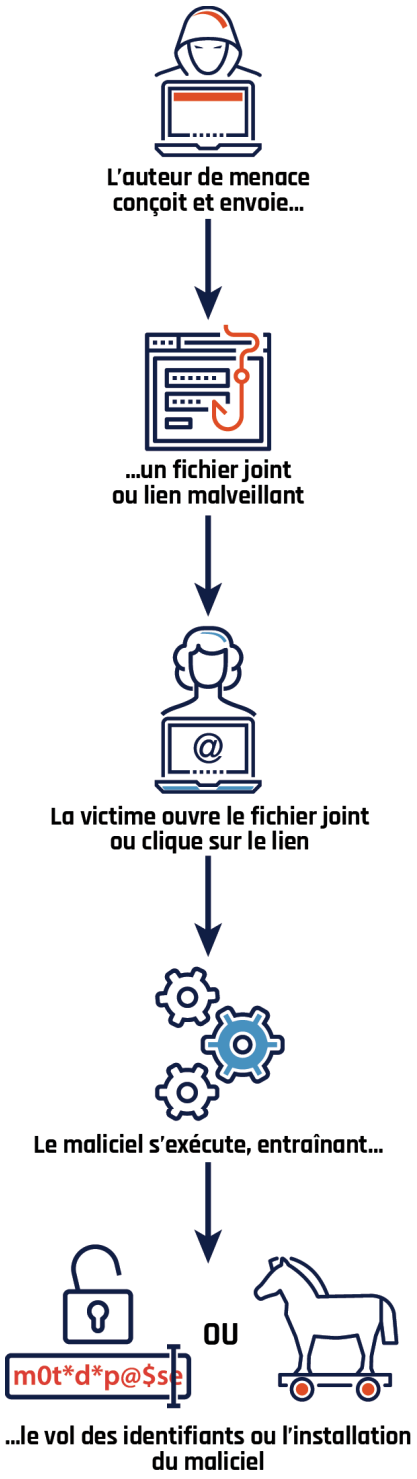


Figure 4 : Hameçonnage et harponnage



HAMEÇONNAGE, MYSTIFICATION, HARPONNAGE, CHASSE À LA BALEINE ET COMPROMISSION DE COURRIEL D'AFFAIRES [Phishing, Spoofing, Spear-Phishing, Whaling, and Business Email Compromise]

L'**hameçonnage** est une technique courante par laquelle les auteurs de menace se font passer pour une entité fiable dans le but d'inciter un grand nombre de destinataires à fournir de l'information les concernant, comme des justificatifs d'ouverture de session, de l'information bancaire et d'autres renseignements nominatifs. L'hameçonnage est une technique de piratage psychologique qui consiste essentiellement à mystifier des courriels et des messages texte. Les utilisateurs tombent dans le piège dès qu'ils ouvrent des pièces jointes malveillantes ou cliquent sur les liens intégrés.

La **mystification** est une technique utilisée pour dissimuler ou falsifier un site Web, une adresse courriel ou un numéro de téléphone de manière à ce qu'il semble provenir d'une source fiable. Après avoir reçu un message d'hameçonnage, la victime peut être invitée à fournir de l'information personnelle, financière ou sensible, ou à cliquer sur un lien ou une pièce jointe, ce qui permettra d'infecter le dispositif en y installant un maliciel.

Le **harponnage** est une technique qui consiste à envoyer un message d'hameçonnage personnalisé à un groupe précis de destinataires ou à un seul destinataire. Basée sur le piratage psychologique, cette technique utilise des détails destinés à convaincre la victime que le message provient d'une source digne de confiance. La **chasse à la baleine** est un type de harponnage qui vise les cadres supérieurs et les autres destinataires de grande notoriété disposant d'autorisations et d'accès privilégiés.

La **compromission de courriel d'affaires** est une technique qui consiste à envoyer un courriel pour convaincre un employé d'une entreprise de transférer directement des fonds aux auteurs de cybermenace. Pour ce faire, ces auteurs se font passer pour des cadres supérieurs ou des tiers de confiance.

INJECTION DE CODE [Code Injection]

L'**injection de code** est une technique qui consiste à insérer du code malveillant dans un programme informatique en exploitant une faille dans les instructions d'une fonction du programme ou dans la façon dont ce programme interprète les données saisies. Les deux techniques d'injection de code souvent utilisées sont **l'injection de script intersites (XSS pour *Cross-Site Scripting*)** et **l'injection SQL (Structured Query Language)**.

- Le script intersites (XSS) est une méthode d'injection de code au moyen de laquelle un auteur de menace insère et exécute un programme malveillant dans une application Web en contournant les mécanismes de validation des données saisies. Le programme malveillant est exécuté dans le navigateur des utilisateurs qui accèdent à l'application Web infectée, permettant ainsi au code inséré par XSS de s'exécuter immédiatement ou d'être enregistré pour une exécution ultérieure.
- L'injection SQL récupère ou modifie le contenu d'une base de données SQL en insérant du code dans des formulaires Web destinés à saisir des données dans les bases de données SQL ou à les interroger. Ces bases de données peuvent contenir des renseignements nominatifs ou de l'information sensible.

LOGICIEL PUBLICITAIRE OU PUBLICIEL [Adware]

Le principal objectif du **logiciel publicitaire** ou **publiciel** est de générer des revenus en affichant des annonces adaptées à l'utilisateur. Par exemple, les logiciels publicitaires basés sur navigateur et sur application recueillent les informations liées aux utilisateurs et aux dispositifs, dont les données de localisation. Les logiciels publicitaires peuvent mener à l'exploitation des paramètres de sécurité, des utilisateurs et des systèmes. Les maliciels, les attaques de l'intercepteur et les logiciels espions sont souvent associés à cet outil.

LOGICIELS ESPIONS OU ESPIOGICIELS [Spyware]

Les **logiciels espions** ou **espiogiciels** sont des logiciels malveillants utilisés pour recueillir et transmettre les activités numériques et les données personnelles de l'utilisateur à son insu et sans sa permission. Ils peuvent être utilisés dans le cadre de plusieurs activités, notamment l'enregistrement de la frappe, l'accès au microphone et à la caméra Web, la surveillance des activités de l'utilisateur et de ses habitudes de navigation, et la capture des noms d'utilisateurs et des mots de passe.

ORDINATEURS ZOMBIES ET RÉSEAUX DE ZOMBIES [Bots and Botnets]

Un **ordinateur zombie**, ou zombie, est un dispositif connecté à Internet (p. ex. des ordinateurs, des appareils mobiles et les dispositifs qui composent l'Internet des objets) et infecté par un maliciel à l'insu du propriétaire, qu'un auteur de menace peut contrôler à distance afin de mener des opérations illicites. Ensemble, ces dispositifs compromis forment un **réseau de zombies** coordonné par un auteur de menace. Les réseaux de zombies se répandent généralement en sondant l'environnement en ligne dans le but de trouver des dispositifs vulnérables susceptibles d'accroître la puissance informatique et d'ajouter de nouvelles capacités. Ils servent à des fins diverses, telles que pour mener une attaque par déni de service distribué (DDoS pour *Distributed Denial of Service*), propager des rançongiciels et des maliciels, lancer des campagnes publicitaires frauduleuses, envoyer des pourriels, détourner le trafic, voler des données, ou encore pour manipuler, enflammer et censurer les médias sociaux et le contenu de plateformes Web de manière à influencer les débats publics.

PERÇAGE DE MOTS DE PASSE [Password Cracking]

Le **perçage de mots de passe** est une tentative d'accéder directement aux comptes. Deux techniques sont communément utilisées : **par force brute** et **par dictionnaire**. L'attaque par force brute consiste à utiliser un nombre exhaustif de mots de passe générés aléatoirement pour tenter d'accéder au compte, alors que l'attaque par dictionnaire teste une liste des mots les plus courants.

PORTE DÉROBÉE [Backdoor]

Une **porte dérobée** est un point d'entrée au système ou à l'ordinateur d'un utilisateur, qui permet de contourner les mesures d'authentification, le chiffrement ou les systèmes de détection d'intrusion. Les auteurs de menace qui disposent d'un tel accès à distance peuvent voler l'information, installer des maliciels ou contrôler les processus et procédures du dispositif. Les portes dérobées sont souvent créées délibérément aux fins de dépannage, d'application de mises à jour logicielles ou de maintenance des systèmes. Les auteurs de menace peuvent utiliser ces portes dérobées légitimes à des fins malveillantes.

Figure 5 : Rançongiciel

PROGRAMME POTENTIELLEMENT INDÉSIRABLE OU APPLICATION POTENTIELLEMENT INDÉSIRABLE [Potentially Unwanted Program or Application]

Les programmes ou les applications potentiellement indésirables (PPI ou API) sont des logiciels perçus comme étant indésirables et pouvant affaiblir la sécurité globale d'un dispositif et porter atteinte à la vie privée de l'utilisateur. Ils sont souvent compris avec d'autres logiciels téléchargés avec le consentement de l'utilisateur.

RANÇONGICIEL [Ransomware]

Un **rançongiciel** est un programme malveillant qui, dans plusieurs cas, permet de bloquer l'accès à un ordinateur ou à un dispositif et d'en chiffrer les données. L'accès aux systèmes et à l'information n'est rendu à l'utilisateur qu'après le versement d'une rançon, généralement une cryptomonnaie comme le bitcoin. Un rançongiciel peut également verrouiller des systèmes de différentes manières, sans faire appel au chiffrement, nuisant ainsi au rendement du dispositif. Les auteurs peuvent menacer la victime de divulguer de l'information sensible, personnelle ou embarrassante la concernant jusqu'au paiement de la rançon. Un rançongiciel est généralement installé au moyen d'un cheval de Troie ou d'un ver déployé par hameçonnage ou sur consultation d'un site Web compromis.

Certains cybercriminels se livrent à des campagnes de rançongiciel de type **chasse au gros gibier**. Ils concentrent ainsi leurs activités sur de grandes organisations (fournisseurs d'infrastructures essentielles, gouvernements ou grandes entreprises), qui doivent éviter que leurs réseaux soient perturbés et qui sont prêtes à payer de lourdes rançons pour rétablir rapidement leurs opérations.

TYPOSQUATTAGE [Typo-Squatting]

Le **typosquattage** est une technique qui consiste à enregistrer des noms de domaines graphiquement apparentés à une adresse de domaine légitime afin de tirer avantage des fautes de frappe faites par les internautes. Basée sur le détournement d'adresses URL, elle permet aux auteurs de menace de rediriger un utilisateur ayant fait une erreur au moment de saisir l'adresse d'un site Web vers un domaine en apparence similaire sous leur contrôle. Le nouveau domaine peut alors servir à installer un maliciel et à obtenir des renseignements nominatifs ou de l'information sensible. Des techniques d'hameçonnage peuvent également être utilisées pour attirer les utilisateurs vers une adresse URL détournée.

VIRUS, VER, CHARGE DE VIRUS ET CHEVAL DE TROIE

[Virus, Worm, Payload, and Trojan]

Les maliciels sont souvent transmis au moyen de virus, de vers et de chevaux de Troie, et ont d'importantes conséquences. Un **virus** est un programme exécutable et reproductible qui insère son propre code dans des programmes légitimes dans le but de causer des dommages sur l'ordinateur hôte (p. ex. en supprimant des fichiers et des programmes ou en corrompant les systèmes d'exploitation et de stockage). Dans sa forme la plus simple, le **ver** est un programme informatique capable de se reproduire par lui-même et de se propager sur d'autres ordinateurs afin de drainer les ressources du système. Comme le virus, il a également la capacité de propager du code de manière à causer des dommages sur son hôte. Ce code est ce qu'on appelle la **charge de virus** (p. ex. la capacité de chiffrer les fichiers d'un rançongiciel et l'installation de portes dérobées sur les systèmes pour obtenir un accès à distance). Un **cheval de Troie** est un programme malveillant qui prend l'apparence d'un programme légitime ou s'intègre à un tel programme. Bien que ses objectifs soient similaires à ceux des virus et des vers, il ne peut se reproduire ou se propager par lui-même.

VULNÉRABILITÉS ET ATTAQUES DU JOUR ZÉRO

[Zero-Day Vulnerabilities and Zero-Day Exploits]

Par **vulnérabilités du jour zéro**, on entend les vulnérabilités non corrigées qui ne font pas partie du domaine public et qui ne sont connues que par quelques personnes. Un exploit tirant avantage d'une telle vulnérabilité est appelé un **exploit du jour zéro**.